Alberto de Elzaburu
Alfonso D Rivera Elzaburu
Miguel A Baz
Enrique Armijo
Germán Burgos
Luis H de Larramendi
Doris Bandín
Roberto Martínez
Antonio Tavira
Antonio Castán
Ignacio D Rivera Elzaburu
Jesús Gómez Montero
Pablo González-Bueno

Argimiro Cadenas
José Mª Álvarez
Javier Cervera
Begoña Larrondo
Heinrich Möhring
Juan Antonio Rubiano
José Manuel Cruz
Luis Beneyto
Xavier Lamíquiz
José Ignacio San Martín
Miguel Ángel Medina
Manuel Illescas
Luis Baz
Ramón Cañizares

S/Your ref

Víctor Carb[redacted]
Enrique Armij[redacted]
Concepción Chacón
Ana Donate
Catherine Bonzom
Juan José Caselles
Fernando Ilardia
Rosa Torrecillas
Laura Alonso
Javier Úbeda-Romero
Pedro Saturio
Luis Soriano
Juan M Sáinz de Marles
Francisco J Sáez
Carlos Morán M
Juan Antonio Romero
Sofía D Rivera Elzaburu

I Arocas
A Vila
A FD Rivera Elzaburu
L Moraleda
G Armijo
M Glez Gordon
C Sanz
M Vázquez
M García Muñoz

N/Our ref

Continuadores de
Julio de Vizcarrondo 1865-1889
F de Elzaburu Vizcarrondo 1880-1921
Alberto de Elzaburu F 1920-1974
Oscar de Elzaburu F 1924-1985
Oficina Vizcarelza Sres Elzaburu

Abogados y Agentes
de Propiedad Industrial

Agentes de Patentes Europeas
European Patent Attorneys

Agentes Europeos de Marcas
ante la OAMI/OHIM Alicante
European TM Attorneys

Ingenieros, Biólogos
Físicos y Químicos

Agente Registrador .ES (ESNIC)
Traductores Jurados

Telegramas: VIZCARELZA
Teléfono: (34) 91 700 9400
Telefax: (34) 91 319 3810
Videoconf: (34) 91 702 0786
Correo-e: elzaburu@elzaburu.es
Pág web: www.elzaburu.es

Miguel Ángel, 21
28010 Madrid, España

EUROPEAN PATENT
OFFICE
Gitschiner Str. 103
D-10969 Berlín
Alemania

JRT/PCT-114

11 February 2004

BY FAX – 00 49 30 25901 840

CONFIRMATION BY COURIER

REPLY TO THE WRITTEN OPINION PURSUANT RULE 66 PCT

Re: International Application No.: PCT/EP02/04865
Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

Dear Sirs:

In response to the first Written Opinion issued on the above application, hereinafter the present application, in which original claims 1 - 24 were objected of not meeting the criteria mentioned in A.33(1)PCT in view of US 2002/012433 A1 and WO 0176297 A1, the following is submitted on behalf of the applicant:

- enclosure with replacement sheets for new Claims 1-25, both corrected and clean text; and
- new specification pages with the new prior art cited above, both corrected and clean text.

The new Claim 1 is an amendment of the old claim 1, now including in the preamble features anticipated by the prior art cited in the International Search Report and, for the sake of clarity, including references to the inventive use of a Point-to-Point layer 2 protocol like a Point-to-Point over Ethernet protocol between the wireless terminal and the Access Controller. These admissible amendments are supported on paragraphs 0046 and 0047 with due regard to the abstract of the present application.

The new claim 2 filed herewith is new and addresses an advantageous process for automatically discovering an Access Controller from the wireless terminal. This admissible amendment is supported on paragraphs 0049 and 0050 of the present application.

The new claim 3 is not amended and corresponds to the old claim 2.

The new claims 4-6 respectively correspond to old claims 3-5, both reinstated and including a reference to a Point-to-Point over Ethernet protocol, following the clarification introduced in the new claim 1. A clerical mistake referring "the step of shifting/establishing.." has been corrected as "a step of shifting/establishing.." to overcome any objection of lacking respective antecedents.

The new claims 7-14 are not amended but for reinstating dependences when applicable, and respectively correspond to the old claims 6-13.

The new claim 15 is based on the old claim 14 wherein the Point-to-Point server is restricted as a Point-to-Point layer 2 protocol (PPPoE) server. This admissible amendment is supported on paragraphs 0049 and 0050 with due regard to Fig. 3 and abstract of the present application.

The new claims 16-25 respectively correspond to old claims 15-24 and are not amended but for reinstating purposes, and for including reference signs for the sake of clarity.

Citations

D1: US 2002/012433 A1

D2: WO 01/76297 A1

Novelty

D1 and D2 disclose quite close teachings to each other, at least, in respect of those network elements and processes relevant for the purpose of the present invention.

D1 and D2 disclose a system where a wireless adapted terminal (MT) can connect to a home mobile network (GSM) through a Wireless IP access network (WISP). The home mobile network being responsible for authenticating the user (MT) whereas the Wireless IP access network allowing the user to access to the Internet network. The wireless terminal, the Wireless IP access network, and the mobile network all communicated with a mobile IP

protocol. The Wireless IP access network requires, however, a SIM-based authentication of the wireless terminal before giving access to public Internet services.

Therefore, the wireless terminal may consist of a laptop computer with a WLAN card, a SIM and a SIM-reader, and can gain access to a Wireless IP access network through WLAN hot spots (Access Points cited on paragraph 0172 of D1 and thus referred in the wording of the present application). The system comprises a Public Access Controller (PAC) for controlling access from the radio access network to the Internet services. This PAC allocates an IP address to the wireless terminal (MT) and authenticates the MT before connection to the Internet is established. The PAC relays authentication messages between the wireless terminal (MT) and an authentication Gateway (GAGW) of the home mobile network (as explained on paragraph 0257 of D1, and on page 9 line 29 to page 10 line 2 of D2). Moreover, the interface between wireless terminal (MT) and PAC as well as the interface between PAC and authentication Gateway (GAGW) they both are an IP based interface, wherein PAC and MT are identified by respective IP addresses from each other, and wherein PAC and GAGW are also identified by respective IP addresses from each other (as explained on paragraphs 0260-0261 of D1, and on page 10 lines 10-19 of D2). The fact that PAC and MT make use of an IP-based protocol makes essential that the wireless terminal (MT) is assigned an IP address from the very beginning (paragraph 0257 of D1, on page 10 lines 26-32 and on page 11 lines 5-12 of D2), this IP address maintained statically even when the MT roams and changes its location (paragraph 0257 of D1, and on page 17 lines 5-10 of D2). Furthermore, this IP address assigned to the MT, along with other information about the authentication mechanism, is sent from the PAC to the MT before having any possibility to establish a secure channel communication. Still further, all the authentication related submissions are exchanged between the GAGW and the MT through the PAC via a suitable authentication protocol running on top of an IP based protocol.

The present application claims a method in a telecommunication system for allowing a SIM-based authentication to users of a wireless local area network who are subscribers of a public land mobile network, the method comprising the steps of:

- a wireless terminal accessing the wireless local area network through an accessible Access Point;

- discovering an Access Controller interposed between the Access Point and the public land mobile network from the wireless terminal;

- carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof;

wherein these challenge-response authentication submissions take place before having provided IP connectivity to the user, and are carried:

- *on top of a Point-to-Point layer 2 protocol between the wireless terminal and the Access Controller; and*

- *on an authentication protocol residing at application layer between the public land mobile network and the Access Controller;*

and the method further comprises a step of offering IP connectivity to the user at the wireless terminal, ***by sending an assigned IP address and other network configuration parameters, once said user has been validly authenticated by the public land mobile network.***

D1 and D2 may effectively anticipate a step of accessing the wireless local area network through an accessible Access Point; a step of discovering an Access Controller interposed between the Access Point and the public land mobile network; and a step of carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, but all these steps are always carried out, in both D1 and D2, over an IP based interface, or on a suitable protocol running on top of the IP based interface.

Neither D1 nor D2 anticipate, however, that these challenge-response authentication submissions take place before having provided IP connectivity to the user, and neither do they that these challenge-response authentication submissions are carried on top of a Point-to-Point layer 2 protocol between the wireless terminal and the Access Controller whilst carried out on an authentication protocol residing at application layer between the public land mobile network and the Access Controller. Moreover, neither D1 nor D2 anticipate a method wherein the step of carrying out a SIM-based authentication of the wireless terminal takes place before a further step of obtaining an IP address assigned to the wireless terminal.

Thereby, it is respectfully submitted that the new claim 1 as filed herewith is novel in view of D1 and D2.

On the other hand, and given that the novel steps in the above method already discussed are carried out by corresponding technical means, namely the Point-to-Point layer 2 protocol (PPPoE) server and client, respectively located in the Access Controller of claim 15 and in the wireless terminal of claim 24, both corresponding technical means must be novel over, and not anticipated by, the teaching in D1 and D2. Likewise, the telecommunication system of claim 25, including the novel Access Controller of claim 15, must be novel as well.

Thereby, it is respectfully submitted that the new claims 1, 15, 24 and 25 as filed herewith are novel in view of D1 and D2, and claims 2-14 and 16-23, being ultimately dependent on claims 1 and 15 respectively, per force must be novel as well.

Inventive Step

Starting from D1 (or D2), the skilled person may arrive to provide (in the wording of the present application, and with reference signs of D1) a method in a telecommunication system for allowing a SIM-based authentication to users (MT) of a wireless local area network (WISP) who are subscribers of a public land mobile network (GSM), the method comprising the steps of:

- a wireless terminal (MT) accessing the wireless local area network through an accessible Access Point (hot spot);

- discovering an Access Controller (PAC) interposed between the Access Point and the public land mobile network from the wireless terminal;

- assigning an IP address to the wireless terminal; and

- carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof; the challenge-response authentication procedure carried out on a suitable authentication procedure through an IP based protocol, wherein wireless terminal and Access Controller identify each other by respective IP addresses.

The present application faces, amongst others, the problem of lack of security caused by assigning an IP address to the wireless terminal in clear form before getting an agreement on applicable ciphering keys, which are obtained while running the authentication process, in order to avoid that a malicious user might initiate well-known attacks by spoofing this IP address, as described on paragraph 0024 of the present application.

Moreover, the present application is aimed to provide a complete encryption path between the wireless terminal (TE) and the Access Controller, so that the assigned IP address is submitted to the terminal through a secure tunneling, as described on paragraphs 0025-0027 with due regard to the abstract of the present application.

Therefore, the present application skips the step of assigning an IP address to the wireless terminal until having carried out the challenge-response authentication procedure.

However, following the teaching in D1 (or D2), a skilled person would not find how challenge-response authentication submissions might be carried out between the wireless terminal and the Access Controller over an IP based protocol without the wireless terminal having an IP address assigned or known by the Access Controller.

To overcome this problem, the present application introduces an Access Controller comprising:

(a) a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal, and arranged for tunneling the challenge-response authentication procedure; and

(b) an authentication protocol residing at an OSI application layer for communicating with the public land mobile network.

And a wireless terminal comprising functionality for acting as a Point-to-Point layer 2 protocol (PPPoE) client and having an Extensible Authentication Protocol on top of this Point-to-Point layer 2 protocol.

Both, Access Controller and wireless terminal thus cooperating to provide a method with the above limitations from D1 (or D2) and where the challenge-response authentication

submissions in the above third step take place before having provided IP connectivity to the user, and are carried:

- *on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller; and*
- *on an authentication protocol residing at application layer between the public land mobile network and the Access Controller;*

and the method further comprises a step of:

- offering IP connectivity to the user at the wireless terminal, by sending an assigned IP address and other network configuration parameters, once said user has been validly authenticated by the public land mobile network.

These new steps, limitations of claim 1, as well as the new features, being limitations of claims 15 and 24, are not cited at all in D1 (and D2), and this is a first criterion not met to establish a *prima facie* case of obviousness.

Apart from that, D1 (and D2) is silent in respect of an additional protection of the assigned IP address submitted to the wireless terminal from the very beginning. There is no motivation from the teaching in D1 (and D2) for a skilled person to arrive to the problems addressed by the present application, and even less to arrive to the present solution. This lack of motivation in D1 (and D2) being a second criterion not met to establish a *prima facie* case of obviousness.

On the other hand, a skilled person does not find any incentive on carrying out the challenge-response authentication procedure before assigning the IP address to the wireless terminal since the authentication procedure cannot be naturally carried out between two entities interfacing with an IP based protocol, without both entities knowing the IP address of each other. This lack of incentive being a third criterion not met to establish a *prima facie* case of obviousness.

Thereby, it is respectfully submitted that the independent claims 1, 15 and 24 as filed herewith are inventive in view of D1, alone or in combination with D2. Moreover, independent claim 25 directed to a system that comprises the Access Controller of claim 23 must be inventive as well; and claims 2-14 and 16-23, being ultimately dependent on claims 1 and 15 respectively, must be inventive as well over the teaching in D1, alone or in combination with D2.

Consequently, it is respectfully submitted that the claims 1 to 25 as filed herewith satisfy the requirements of A.33(2) PCT, A.33(3) PCT, A.6 PCT, and R.6(3) PCT. Thereby, a favourable reconsideration is hereby requested. Should the examiner is of the opinion that further objections may arise, and in view that the term until the IPER must be established

will not expire until the 1st of September 2004, issuance of a second Written Opinion is hereby also requested, allowing the applicant to file a response thereto.

Yours sincerely,

ELZABURU

Alberto de Elzaburu, P.P.

Enclosures:

- Replacement sheets for new claims 1-25, both corrected and clean text.
- New Specification pages with the new prior art cited above, both corrected and clean text.